

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

In the Matter of the Search of:)	
)	Case No: 2:22-mj-734
Information, including the content of communications)	
associated with the Snapchat account for username)	Magistrate Judge: Deavers
“hunter2596” (SUBJECT ACCOUNT),)	
that is stored at the premises controlled by Snap, Inc.)	<u>UNDER SEAL</u>

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI),
being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including the online exploitation of children.
2. During my career as a police and task force officer, I have participated in hundreds of investigations regarding computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses and child exploitation. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252(a), 2252A, 2251 and 2422.
3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat Screen/Username that is stored at premises owned, maintained, controlled, or operated by Controlled by Snap, Inc. ("Snapchat"), a social networking company headquartered at 2772 Donald Douglas Loop North, in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snapchat to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Screen/Username: hunter2596 (the **SUBJECT ACCOUNT**).
5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers, agents, and witnesses. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the **SUBJECT ACCOUNT**. I have not omitted any facts that would negate probable cause.
6. The **SUBJECT ACCOUNT** to be searched is more particularly described in Attachment A, for items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the production, receipt, distribution, transportation, advertisement, or possession of child pornography. I am requesting authority to search the entire content of the **SUBJECT ACCOUNT**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

7. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed,

or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce.

Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
10. The term "child pornography", as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.

11. The term “sexually explicit conduct”, as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as “actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.” Pursuant to 18 U.S.C. § 2256(2)(B), “sexually explicit conduct” when used to define the term child pornography, also means “(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.”
12. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
13. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.
14. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
15. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
16. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic

“address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

17. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
18. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

IV. BACKGROUND INFORMATION REGARDING SOCIAL MEDIA AND SNAP

19. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and conversations with other officers, I know the following:
20. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol

addresses and other information both in computer data format and in written record format.

21. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
22. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, Kik messenger service, Snapchat, Meet24, and Instagram.
23. According to the Snap Law Enforcement Guide, "Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats." Snapchat's differentiating feature from other communications applications is that a sender is able to set a variable amount of time the message is viewable by the receiver. This time can be between one and ten seconds. At the expiration of time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices. If the receiver of a Snapchat message does not access the application on their device, the message remains undelivered. Snap's services are designed to store unopened snaps for 30 days. After 30 days the messages are deleted from Snap's servers.
24. Snapchat users have the following abilities:
 - ☐ Snaps: photos or videos taken using his or her phone's camera (or the Snapchat app's camera), which may be shared directly with the user's friends, or in a Story (explained below), or Chat. Snaps can also be sent from the saved pictures/videos in

the gallery of the device. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it is opened in the case of the recipient). Users are able to save a photo or video they've taken locally to their device or to Memories, which is Snapchat's cloud-storage service.

- **Stories:** A user can add photos or videos (Snaps) to their "Story." A Story is a collection of Snaps (*i.e.*, photos or videos) displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to Snap's crowd-sourced service "Our Story," which enables their Snaps to be viewed by all Snapchatters in search and Snap Map. Snap's servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.
- **Memories:** Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case content is not accessible to Snap and cannot be decrypted by Snap.
- **Chat:** A user can also type messages, send photos (Snaps), audio notes, and video notes to friends within the Snapchat app using the Chat feature. Snap's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again. This will result in it being deleted from Snap's services. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not.

- Location Data: If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

25. Information that Snapchat possesses and maintains:

- Personal Identifying Information: When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. A user also enters a date of birth. This is supposed to prevent anyone under the age of 13 from using Snapchat. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.
- Usage Information: While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains log files and information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.
- Device Information: Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat.
- Device Phonebook and Photos: If a user consents, Snapchat can access from their device's electronic phonebook or contacts list and images.

- Location Data: may be available for a Snapchat user who has turned on location services on their device and opted into location services in the app settings.
 - Message Content: Because Snap’s servers are designed to automatically delete most user content, and because much of a user’s content is encrypted, Snap often cannot retrieve user content except in very limited circumstances. For example, Memories content may be available until deleted by a user.
26. If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user’s use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.
27. Therefore, the computers/servers of Snapchat are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat, such as account access information, transaction information, and other account information.

VII. INVESTIGATION AND PROBABLE CAUSE

28. On June 17, 2022, law enforcement officers with the Licking County Sherriff’s Office (LCSO) received a report indicating that John Doe One, a sixteen-year-old male, was offered money and other gifts in exchange for engaging in sexual acts with an adult male. In conducting an investigation into these allegations, LCSO contacted John Doe One who then participated in a forensic interview on June 27, 2022. During that interview, John Doe One revealed that Matthew Reif (REIF) had shown him adult pornography and pornography involving minor children on multiple occasions over the last two years. More specifically, LCSO learned that John Doe One and the family of John Doe One knew REIF through their association with the Heath Church of Christ located in Heath, Ohio. John Doe One also revealed that REIF asked him for photos of his erect penis. In addition, John Doe One advised that REIF had solicited nude photos of other juvenile males that both he and REIF were acquaintances with. More specifically, John Doe One identified a juvenile relative of REIF and indicated that REIF’s relative had once disclosed to John Doe One that REIF had taken his nude photos in the past.
29. That same day, as a follow-up to the interview with John Doe One, an interview with

REIF was conducted by the LCSO. During that interview, REIF admitted to offering John Doe One money and other gifts, including Jordan tennis shoes, in exchange for John Doe One allowing REIF to engage in acts of masturbation with him. REIF further admitted that he had solicited two other male juveniles for photos of their penises and that those images were sent to REIF in exchange for REIF sending the juvenile's money and gifts. REIF noted that these conversations with the juvenile males, including John Doe One, occurred primarily via text message and the mobile application, Snapchat. Furthermore, REIF acknowledged to law enforcement with the LCSO that he utilized the email addresses matt17reif@gmail.com and djlittlemattie@gmail.com.

30. On or about July 1, 2022, REIF was arrested by the LCSO for violations of the Ohio Revised Code (ORC) relating to Pandering Obscenity Involving a Minor (2907.32) and Illegal Use of a Minor in Nude Oriented Material (2907.323).
31. On or about July 6, 2022, search warrants seeking to seize digital media devices belonging to REIF were executed by LCSO. Several digital media devices, including a Puanv USB drive, Micro SD cards, Apple iPad, and an Apple Macbook were recovered pursuant to those warrants.
32. The investigation by LCSO further revealed that REIF was employed as a travelling surgical technician which required him to commute for work. More specifically, law enforcement learned that REIF drove to Indiana for work and commuted back and forth between Ohio and Indiana for his job. In doing so, REIF maintained a residence at 140 Greer Drive in Newark, Ohio on the weekends and during the week, resided at 222 Forest Drive in Jeffersonville, Indiana. On July 5, 2022, an additional search warrant was obtained for REIF's Jeffersonville, Indiana address by the Indiana State Police. As a result of that search warrant, numerous digital media devices were seized to include two digital cameras, an Apple Macbook, Apple iPad, and iPhone, SD cards, and a hard drive.
33. During the seizure processes of the digital media devices belonging to REIF, LCSO began to preliminarily review the potential evidence contained on them. A cursory review of the Puanv USB drive seized from REIF's vehicle revealed numerous file folders, each of which was identified with the name of a male as the file folder title. Contained within each individual folder were videos which depicted different males, both juvenile and adult, engaged in acts of masturbation. In addition, a number of videos and images saved within the folders appeared to have been created via the Snapchat app.

34. Through further investigation, law enforcement with the LCSO learned that many of the males depicted within these folder files were local to the Newark, Ohio area and began attempting to identify the males based on their name and/or images and/or saved files. Although the investigation is still ongoing at this time, approximately a dozen males who have been identified thus far admitted to distributing photos or videos of themselves nude and/or masturbating via Snapchat when they were between the ages of fourteen and seventeen years of age. Although a majority of these males advised they knew REIF, they all separately believed that they were communicating on Snapchat with a female named Nicole Smith when they distributed image and videos of themselves on Snapchat. LCSO further noted that the Snapchat videos and images recovered from REIF's Punav USB drive depicted Snapchat conversations between a male and a purported female who used a female name and female emoji while communicating. It is believed, based on the investigation thus far, that REIF utilized a female persona on Snapchat to communicate and make contact with the juvenile males, eventually soliciting child sexual abuse material from them, recording that content, and saving it to his USB drive.
35. Further review of two additional SD cards revealed a video of John Doe One masturbating in a shower. LCSO reviewed the video and noted that REIF was in the video and observed placing the camera in the shower. After the camera was placed, John Doe One was depicted entering into the shower and masturbating. After the recovery of this video, John Doe One participated in a second interview, during which, John Doe One admitted that he had gone to a hotel located in Hebron, Ohio with REIF on approximately five to seven occasions when he was fifteen years of age. According to John Doe One, REIF "bribed" him to masturbate in the shower, however, John Doe One stated he was unaware that he was being recorded by REIF at the time.
36. An arrest warrant for REIF was issued by U.S. Magistrate Judge Kimberly A. Jolson on August 12, 2022 pursuant to a criminal complaint for the Sexual Exploitation of a Minor as well as Receipt, Distribution, and Possession of Child Pornography. REIF was then taken into federal custody and arraigned.
37. On September 13, 2022, REIF agreed to a proffer with your affiant and members of the United States Attorney's Office in Columbus, OH. That proffer continued into a second interview that was held with REIF on September 30, 2022 at the Franklin County Correction Center II in Columbus, Ohio. During these conversations with REIF, REIF

provided information relating to another child exploiter. More specifically, REIF indicated that his personal friend, Justin Kling (KLING), had been involved in the production and receipt of child pornography.

38. Your affiant further learned that REIF and KLING had conversations via text message and Snapchat within the last twelve months, during which, they both discussed their sexual interest in children. REIF confirmed to your affiant that he distributed files of child pornography to KLING at KLING's request via Snapchat and that those images depicted prepubescent males and females. REIF stated that KLING inquired as to how REIF obtained these images but was very cautious about evidence of his child exploitation interests being found on his cellular phone. In addition, REIF indicated that he also sent a Mega link to KLING via Snapchat which contained files of child pornography. REIF recalled that KLING asked how to access the link and REIF explained that he had to download the Mega app to his phone which REIF believes KLING did to access the files.
39. In continuing the conversation regarding their shared interest in child pornography, your affiant learned that REIF asked KLING if KLING had any files of child pornography. In response, KLING sent REIF an image depicting a nude prepubescent female's vagina. KLING asked REIF if he had taken the photo and KLING acknowledged that he had but would not tell REIF who the child was at that time.
40. Your affiant further learned from REIF that KLING had previously resided with a married couple who had three prepubescent daughters living with them inside the residence (herein after VICTIM FAMILY). According to REIF, when KLING verified that he had taken the child pornography image, REIF assumed that the child who was a member of VICTIM FAMILY that KLING had previously resided with in Alexandria, Ohio.
41. According to REIF, KLING eventually stated that KLING took nude photos of at least one of the prepubescent daughters in the VICTIM FAMILY while they were sleeping and had also attempted to digitally penetrate at least one of the girls. Your affiant learned that both KLING and REIF were apprehensive about sending child pornography files via Snapchat so, when they were together, they would show each other photos on their phones. Your affiant learned from REIF that he believed KLING showed REIF additional images depicting nude images of the children in the VICTIM FAMILY, but REIF could only specifically remember the one described above.
42. REIF advised your affiant that he told KLING about the recorded videos of John Doe One

and further shared several of these videos with KLING. According to REIF, KLING was aware of the age of John Doe One in the videos. Prior to showing KLING the videos, REIF asked KLING if he wanted to see them at all and REIF stated that he asked KLING this because KLING was interested in much younger children than REIF was and John Doe One was older than KLING's preferred age.

43. After speaking with REIF about KLING, your affiant worked to corroborate any of the information provided by REIF from the forensic devices your affiant had obtained related to the initial investigation of REIF. Recovered in the forensic extraction of REIF's Apple iPhone 11 was a text conversation between REIF and KLING occurring from approximately September 24, 2021, to October 8, 2021.
44. Your affiant would note that on September 28, 2021, REIF and KLING engaged in a text message conversation, during which, they discussed engaging in sexual intercourse together in conjunction with an eighteen-year-old female. The following conversation then ensued:

REIF:	"Would you fuck a 16 yo lol"
KLING:	"Fuck yeah if I can't get caught"
REIF:	"Haha any younger?"
KLING:	"Maybe depends I guess would u lol"
REIF:	"This all between us?"
KLING:	"Yes"
KLING:	"Of course"
REIF:	"What's the youngest you would fuck"
KLING:	"Maybe 13 or 14"
REIF:	"Damnnn a 13 year old?"
REIF:	"Ok"
KLING:	"Maybe. If she's right for it. Tight Pussy. Hbu"
KLING:	"I ain't no saint bro."
REIF:	"Well between us. Def would fuck 12 or older haha"
REIF:	"Super friggin tight"
REIF:	"This has gotta stay with us tho or we could get in big trouble lol"
KLING:	"No shit"
REIF:	"Lmao. 13 the youngest?"
KLING:	"No I'd probably"
REIF:	"Haha can u imagine if we 3 somed a 12 year old"
REIF:	"Insane"
KLING:	"Savage. Bro fucking savage"
REIF:	"Would u be down to tear a kid up"
KLING:	"If some young girl txted and was like let's fuck if he like when and where"
REIF:	"For sure. What would you take thw mouth or the pussy"
REIF:	"Lol"

REIF: "Should we text about this kinda stuff on snap so it's not saved on phone records?"
KLING: **"Both. U got to change it up."**
REIF: "Haha true true"
KLING: **"I'm going to delete all this."**

REIF: "Am I the only one I text like this? Haha and me too. We can continue on snap"
REIF: "U"
REIF: "Why aren't U texting me back on snap"
REIF: "Or is it glitched"
KLING: **"I'm driving"**
REIF: "Sorry lmao"
REIF: "Gotta surprise on snap"
REIF: "U busy?"
REIF: "Check snap if you're not busy"
KLING: **"Ok. Give me a minute"**
REIF: "I kind a like we can talk like this, do you agree?"
KLING: **"Yes"**
REIF: "Cool haha I'm free all night"

45. Your affiant then observed a text from REIF to KLING on September 29, 2021, in which REIF stated, "Surprise on snap". On September 30, 2021, the following text conversation continued:

KLING: **"Dude did u delete ur Snapchat? Your is gone from my list"**
REIF: "It got deleted. Guess I sent u too much stuff"
KLING: **"What!"**
REIF: "Yeah. Got an email from Snapchat saying I violated their terms and so my account got deleted"
KLING: **"Damn"**
REIF: "Yep"
REIF: "Oh well maybe it was for the best"
KLING: **"Didn't u have like 1000 person streaks too"**
KLING: **"Maybe"**
REIF: "Well that ended a while ago"
REIF: "I wanted to get rid of snap anyways"
REIF: "I'd delete anything U have"
KLING: **"It got rid of everything I got nothing"**
REIF: "That's good. I need to as well"
REIF: "It's a good thing it's deleted"

46. During further investigation, law enforcement learned that two separate CyberTipline reports involving REIF were submitted to the National Center for Missing and Exploited Children (NCMEC): CyberTip #103077083 (herein after referred to as CyberTip One) and

CyberTip #103317742 (herein after referred to as CyberTip Two).

47. More specifically, law enforcement learned via CyberTip One that, on the evening of September 28, 2021 (EST), two files of suspected child sexual abuse material had been distributed on Snapchat by the Snapchat screen/username “lildudematt”. Those two files were both videos, one of which depicted an adult male inserting his penis into the anus of a prepubescent male. The second video file depicted a prepubescent female exposing her vagina and then engaging in acts of masturbation. According to information provided by Snapchat, the email address associated to the “lildudematt” account was noted as matt17reif@gmail.com. In addition to the above information, CyberTip One provided the following information related to the “lilmattdude” Snapchat user:

Date of Birth:	11-01-1995
IP Address:	107.77.235.219
	09/30/21 :20:56 UTC

48. Law enforcement also reviewed CyberTip Two and noted that on the evening of September 29, 2021 (EST), the day after the incident date from CyberTip One, four files of suspected child sexual abuse material had been uploaded to Snapchat by the screen/username “lildudematt”. Two of those files were videos, one of which depicted a nude prepubescent female engaged in acts of masturbation. A second video depicted a prepubescent female nude from the waist down. The prepubescent female was observed masturbating. According to information provided by Snapchat for CyberTip Two, the email address associated to the “lildudematt” account was again noted as matt17reif@gmail.com. In addition to the above information, CyberTip Two also provided the same user date of birth and IP address information as noted above in CyberTip One. Your affiant would further note that these two CyberTip reports correspond to the text message exchange between REIF and KLING as noted above.
49. On September 19, 2022, your affiant traveled to the residence of the VICTIM FAMILY and made contact with one of the adult members of the VICTIM FAMILY. Your affiant confirmed that three prepubescent females, between the ages of six years old through twelve years old, and one prepubescent male resided in the house. Your affiant also learned that KLING had in fact resided with VICTIM FAMILY from approximately 2017 to 2019 and that KLING would babysit the children at times, read them bedtime stories, and put them to bed. Your affiant learned that the adult members of the VICTIM

FAMILY were not aware of any inappropriate behavior involving KLING or any of the children and that the VICTIM FAMILY was still friends with KLING and KLING's parents. In addition, your affiant learned that KLING was at the residence of VICTIM FAMILY a few weeks earlier and told VICTIM FAMILY he was residing at 803 Colonial Drive in Heath, Ohio with his parents.

50. On October 11, 2022, a search warrant was executed at 803 Colonial Drive, Heath, OH 43056 which was determined to be KLING'S residence. KLING was not present at the time the search warrant was executed and your affiant later learned that he was in Florida visiting family. Several pieces of digital media were seized from KLING'S bedroom at the time of the search warrant including an older model Apple iPhone. Pursuant to the federal search warrant to forensically examine devices seized attributed to KLING, the iPhone recovered from KLING's bedroom was analyzed. That search revealed a Snapchat account for KLING in which he was utilizing the Snapchat account with the username "hunter2596" the **SUBJECT ACCOUNT**.

51. Based on the information that has been gathered to date by your affiant, your affiant has reason to believe that the individual utilizing the **SUBJECT ACCOUNT**, Justin KLING, has produced, distributed and/or received child pornography. Therefore, it is likely that the **SUBJECT ACCOUNT** contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A,— the production, distribution, transmission, receipt, and/or possession of child pornography.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

52. Based on my own knowledge, experience, and training in online child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in minors and/or seek to sexually exploit minors via online communications:

- A. Those who have a sexual interest in minors, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from discussions of or literature describing such activity.

- B. Those who have a sexual interest in children and/or seek to sexually exploit minors via online communications may collect sexually explicit or suggestive materials in a variety of media. These materials are frequently used for the sexual arousal and gratification of the individual. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
 - C. Individuals who have a sexual interest in children have been found to: download, view, then delete child pornography on a cyclical and repetitive basis; view child pornography without downloading or saving it; or save child pornography materials to cloud storage.
 - D. Those who have a sexual interest in minors may correspond online with and/or meet others to share information about how to find child victims, exchange stories about their sexual exploits with children, and/or exchange child pornography materials; and tend to conceal and maintain in a safe, secure and private environment such correspondence as they do any sexually explicit material related to their illicit sexual interest.
 - E. When communications relating to a sexual interest in children, and/or child pornography files are stored on or accessed by computers and related digital media, forensic evidence of the accessing, downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such files have been deleted from the computers or digital media.
53. Based upon the conduct of individuals who have a sexual interest in children and/or seek to sexually exploit minors via online applications and platforms, as set forth in the above paragraphs, there is probable cause to believe that evidence of the offenses of production, receipt/distribution and possession of child pornography is currently located on the **SUBJECT ACCOUNT**.

IX. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

54. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap Inc. to disclose to the government copies of the records and other

information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.



X. CONCLUSION

55. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the production, distribution, transmission, receipt, and/or possession of child pornography is located in the content of the **SUBJECT ACCOUNT**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNT** described in Attachment A, and the seizure of the items described in Attachment B. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNT** described in Attachment A, and the seizure of the items described in Attachment B.
56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,


Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 10th day of November, 2022.


Elizabeth A. Preston Deavers
United States Magistrate Judge


ATTACHMENT A
ITEMS TO BE SEARCHED

This warrant applies to information associated with the Snapchat Username: hunter2596, which is the subject of preservation requests sent to Snap, Inc., on October 21, 2022 that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop, North Santa Monica, CA 90405.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Snap Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap Inc. (“Snapchat”), including any text, image or video messages, records, files, logs, or information that have been deleted but are still available to Snapchat, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for each user name listed in Attachment A, from September, 2021 to July, 2022.

(a) All Basic subscriber information may including:

- a. Snapchat username
- b. Email address
- c. Phone number
- d. Display name
- e. Snapchat account creation date and IP address
- f. Timestamp and IP address of account logins and logouts

(b) All photos or videos taken using Snapchat’s app’s camera, and/or shared with the user’s friends, or in a Story or Chat, including metadata associated with such images or videos.

(c) All Stories sent from the account identified in Attachment A to any other Snapchatters, the user’s friends, or the user’s custom audience.

(d) All text and multimedia messages stored and presently contained in, or on behalf of the account or identifier;

(e) All Snaps viewed by all Snapchatters in Search and Snap Map.

- (f) All Memories stored in Snapchat's cloud-storage service, to include all sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories.
- (g) All user typed messages, Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature.
- (h) All opened and Unopened one-to-one Chats in to include Chats sent in groups.
- (i) All User saved messages.
- (j) All Device-level location services maintained by Snapchat.
- (k) All activity logs for the account and all other documents showing the user's posts and other Snapchat activities;
- (l) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (m) All "check ins" and other location information;
- (n) All IP logs, including all records of the IP addresses that logged into the account;
- (o) All past and present lists of friends created by the account;
- (p) All records of Snapchat searches performed by the account;
- (q) The types of service utilized by the user;
- (r) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (s) All privacy settings and other account settings, including privacy settings for individual Snapchat posts and activities, and all records showing which Snapchat users have been blocked by the account;

- (t) All records pertaining to communications between Snapchat and any person regarding the user or the user's Snapchat account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the production, receipt, distribution, transportation, advertisement, or possession of child pornography

- (a) Evidence indicating how and when the Snapchat account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Snapchat account owner;
- (b) Evidence indicating the Snapchat account owner's state of mind as it relates to the crime under investigation; pertaining to the production, possession, receipt, coercion, enticement or distribution of child pornography and child erotica.
- (c) Evidence of communications related to the production, possession, receipt, or distribution of child pornography and/or, the coercion or enticement of a minor to engage in illegal sexual activity.
- (d) Evidence the user possessed, exchanged or requested visual depictions of minors, from other adults or minors themselves, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
- (e) Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.